STATE OF MONTANA
DEPARTMENT OF CORRECTIONS
POLICY DIRECTIVE

Policy No. DOC 1.7.6	Subject: **UNLAWFUL USE OF COMPUTERS**
Chapter 1: ADMINISTRATION AND MANAGEMENT	Page 1 of 4
Section 7: Information Systems	Effective Date: Dec. 1, 1996
Signature: /s/ Mike Ferriter, Director	Revised: 04/26/07 Reviewed: 12/15/08

I. POLICY

The Montana Department of Corrections requires all state-owned computer equipment or software to be operated lawfully and in compliance with all applicable state statutes.

II. APPLICABILITY

All divisions, facilities, or programs under Department jurisdiction or contract.

III. DEFINITIONS

Computer Use – As used in *§ 45-6-311, MCA*, the term "obtain the use of" means to instruct, communicate with, store data in, retrieve data from, cause input to, cause output from, or otherwise make use of any resources of a computer, computer system, or computer network or to cause another to instruct, communicate with, store data in, retrieve data from, cause input to, cause output from, or otherwise make use of any resources of a computer, computer system, or computer network.

Computer Virus – A dangerous computer program with the characteristic feature of being able to generate copies of itself, and thereby spreading. Additionally, most computer viruses have a destructive payload that is activated under certain conditions.

IV. DEPARTMENT DIRECTIVES

A. General Prohibitions

1. A person commits the offense of unlawful use of a computer if the person knowingly or purposely:

   a. obtains the use of any computer, computer system, or computer network without consent of the owner;
   b. alters or destroys or causes another to alter or destroy a computer program, computer software or data without consent of the owner; or
   c. obtains the use of or alters or destroys a computer, computer system, computer network, data, or any part thereof as part of a deception for the purpose of obtaining money, property, information, or computer services from the owner of the computer, computer system, computer network, or part thereof or from any other person.

B. Virus Introduction

1. Users will not knowingly introduce a computer virus into a state computer.

2. Prior to introduction into any state computer, users must conduct a virus scan on ALL removable media that has been used any place other than their own workstation.

C. Prohibited Uses of State Computer Resources

1. Using state computer resources to create, access, download, or disperse derogatory, racially offensive, sexually offensive, harassing, threatening, or discriminatory materials.

2. Down-loading, installing, or running security programs or utilities, which reveal or could be used to reveal weaknesses in the security of the state's computer resources, unless your job specifically requires it and it has been approved by the CIO.

3. Use of computers, computer systems, networks or User IDs without the consent of the Department’s security officer.

4. Attempting to modify, install, or remove state computer equipment, software, or peripherals without proper authorization. This includes installing any hardware or software on state-owned equipment.

5. Accessing computers, computer software, computer data or information, or networks without proper authorization, regardless of whether the computer, software, data, information, or network in question is owned by the state, i.e., if you abuse the networks to which the state has access or the computers at other sites connected to those networks, the state will treat this matter as an abuse of your computing privileges.

6. Circumventing or attempting to circumvent normal resource limits, logon procedures, and security regulations.

7. The use of computers, User IDs, or computer data for purposes other than those for which they were intended or authorized.

8. Sending fraudulent e-mail, breaking into another user's e-mailbox, or unauthorized personnel reading someone else's e-mail without his or her permission.

9. Sending any fraudulent electronic transmission including. but not limited to, fraudulent requests for confidential information, fraudulent submission of electronic purchase requisitions or journal vouchers, or fraudulent electronic authorization of purchase requisitions or journal vouchers.

10. Violating any software license agreement or copyright, including copying or redistributing copyrighted computer software, data, or reports without proper, recorded authorization.

11. Taking advantage of another user's naiveté or negligence to gain access to any User ID, data, software, or file that is not your own and for which you have not received explicit authorization to access.

12. Physically interfering with other users' access to the state's computing facilities.

13. Encroaching on or disrupting others' use of the state's shared network resources by creating unnecessary network traffic, e.g., playing games; wasting computer time, connect time, disk space, or other resources; modifying system facilities, operating systems, or disk partitions without authorization; attempting to crash or tie up a state computer; damaging or vandalizing state computing facilities, equipment, software, or computer files.

14. Disclosing or removing proprietary information, software, printed output or magnetic media without the explicit permission of the owner.

15. Reading other users' data, information, files, or programs on a display screen, as printed output, or via electronic means, without the owner's explicit permission.

16. Knowingly transferring or allowing to be transferred to, from or within the agency, textual or graphical material commonly considered to be child pornography or obscene as defined in *§ 45-8-201(2), MCA.*

17. Any use for private or commercial profit.

18. Any use for product advertisement or political lobbying.

19. Downloading any confidential or personally identifiable information to any removable storage media that is not Department owned AND is not encrypted.

20. Sharing, giving, or selling Department owned confidential or personally identifiable information with anyone outside of the agency without explicit permission.

D. Reporting Unlawful Use

1. Users will report unlawful use and other security violations to their immediate supervisor, to local personnel responsible for local network policy enforcement, or to personnel responsible for the security and enforcement of network policies where the violation originated.

2. The Human Resource Bureau will report all employee suspensions, resignations, and terminations to the IT security officer as soon as the event takes place. The security officer will suspend the employee’s accounts, thereby preserving evidence for investigation.

E. Disciplinary Action

1. If, following an investigation, it is determined that an employee has violated this policy, the result may be immediate termination of network and system access.

2. Violators may be subject to disciplinary action up to and including termination under *DOC Policy 1.3.2, Employee Performance and Conduct Guidelines.* Further, in some cases the severity of the violation may mandate that it be reported to the state’s cyber security officer and the state’s CIO. Once the reported violation reaches this level, it may involve the attorney general and legislative auditor’s office.

F. Legal Action

1. In the event that a Department employee is believed to have been involved in the unlawful use of a computer, the Department will pursue an investigation in accordance with *DOC Policy 3.1.19, Investigations.*

V. CLOSING

Questions concerning this policy should be directed to the Chief Information Officer or the IT Policy and Strategic Planning Officer.

VI. REFERENCES

A. ENT-SEC-102 Enterprise IT Policy
B. 2-15-114, MCA (2007) Security Responsibilities of Departments for Data; 2-17-534, MCA (2007) Security Responsibilities of Department; 45-6-310, MCA (2007) Definition – Computer Use; 45-6-311, MCA (2007) Unlawful Use of a Computer; 45-8-201, MCA (2007) Obscenity
C. 1-0243.40; Montana Operations Manual
D. DOC Policies 1.3.2, Employee Performance and Conduct Guidelines; 3.1.19, Investigations

VII. ATTACHMENTS

None.